IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	8:07CR199
	)	
HAROLD STULTS,	)	
	)	
Defendant.	)	

UNITED STATES' BRIEF IN RESPONSE TO THE MOTION TO SUPPRESS

Prepared and Submitted by:

JOE W. STECHER
United States Attorney

and

MICHAEL P. NORRIS (#17765)
Assistant U.S. Attorney
1620 Dodge Street, Suite 1400
Omaha, NE 68102-1506
(402) 661-3700

Nature of the Case.

Harold Stults is charged with possessing one or more photographs and other matter which contain an image of child pornography that had been mailed and shipped and transported in interstate commerce by any means, including by computer, in violation of Title 18, United States Code, Section 2252(a)(4)(B). The Grand Jury returned the indictment on May 23, 2007. Stults filed a motion to suppress all evidence obtained from him as a result of the search warrant issued on his residence. Stults challenged the facial validity of the warrant. A hearing was held on August 14, 2007, wherein the search warrant was received into evidence. (Exhibit 1).

During the hearing, the court allowed Stults to expand his motion. Stults has now filed a supplemental motion to suppress contending that the file sharing by Special Agent Cecchini was, in essence, a warrantless search conducted without the consent of Stults. The United States respectfully submits that the supplemental motion to suppress should be denied. Stults does not have an expectation of privacy in files that he allows to be shared by the general public. By allowing the general public access on a peer-to-peer file sharing network, Stults cannot be heard to complain when one of the file sharers turns out to be a law enforcement officer.

Facts.

Exhibit 1, the search warrant for 8042 Maywood Street, Omaha, Nebraska, sets forth probable cause for the authorization of the search warrant. Paragraphs 6(C) through 6(I) set forth the use of Peer-to-Peer (P2P) file sharing networks and their use in the distribution and sharing of child pornography. P2P file sharing is a method of communication available to Internet users through the use of special software. That software allows users to trade digital files through a worldwide network that is formed by linking computers together. (¶ 6(C))

To access a P2P network, a user first obtains P2P software, which can be downloaded from the Internet. This is done exclusively for the purpose of sharing digital files. All files that a user places in a “shared” folder are available to anyone on the world-wide network for download. The more files that an individual allows to share affects the user’s ability to download files. This is done to encourage users to share their files. (¶ 6(D)).

A user obtains files by conducting keyword searches of the P2P network. The results of the keyword search are displayed and the user may then select files from other users which he/she wants to download. The download of a file is achieved through a direct connection between the computer requesting the file and the computers hosting the file. Once downloaded, the files are stored in the area previously designated by the user and will remain there until moved or deleted. (¶ 6(E)).

A person interested in sharing child pornography with others in a P2P network need only place those files in his/her shared folders. Those child pornography files are than available to all users of the same P2P network. For instance, a person interested in obtaining child pornography can open the P2P application on his/her computer and conduct a keyword search for files using a term such as “preteen sex.” This search would return results of files being shared on the P2P network that matched the term “preteen sex.” The user can then select files from the search results and download directly from the computer sharing those files. (¶ 6(F)). One does not have the ability to send files from his/her computer to another user’s computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user’s computer without his/her active participation. (¶ 6(I)).

The Summary of Investigation section of the Affidavit, paragraphs 23 and 24, set forth the interaction between Special Agent Joseph Cecchini of the Federal Bureau of Investigation's computer and Stults' computer. On October 26, 2006, Agent Cecchini, connected to the Internet in an undercover capacity, and signed on to the P2P file sharing program LimeWire. Agent Cecchini conducted a search using the term "pthc," which is known to be associated with images of child pornography. (pthc is a common abbreviation for preteen hardcore). Among the responses to the "pthc" search term was a computer later determined to be Stults'. Agent Cecchini initiated several downloads from Stults' files that bore file names consistent with child pornography. Those files and the descriptions associated with the files are set forth in the affidavit. A review by the affiant to the search warrant confirmed that at least three of the images were, in fact, child pornography.

Argument.

"LimeWire is a popular Peer-to-Peer file sharing program that permits computer users to distribute and receive photographs, videos and music over the Internet. Once a user installs LimeWire's file sharing software and designates files as being available for sharing, other distant LimeWire users can access and download those files. Although it is capable of being used for legitimate purposes, LimeWire also permits large-scale dissemination of child pornography." United States v. Sloan, 2007 WL 1521434 (D.Hawaii). See also, Wikipedia, LimeWire.

There are other peer-to-peer file sharing programs available to the public. Included on the Gnutella Network are Morpheus, Bearshare, LimeWire, Notella, Gnucleus, and similar systems such as KaZaA and Grokster. Advanced Peer-Based Technology Business Models, a new economic framework for the digital distribution of music, film and other intellectual property works. Massachusetts Institute of Technology Sloan School of Management, 2002.

A peer-to-peer system is designed so that the end user (Stults) has to tell the software that he has downloaded what he will allow to be shared on the system. An agent may not gain access to more of the computer than what the suspect has allowed for the public to access. Anyone downloading from the user (Stults), whether he be an undercover agent or another P2P user, can access the same material. If Stults did not register and download LimeWire, his files would not be accessible by the agent or other LimeWire users.

Stults simply cannot have an expectation of privacy on files that he grants access to and shares with the general public. One would no more expect a shopkeeper who sells contraband to assert an expectation of privacy when a plainclothes police officer enters the shop, makes a purchase, and later returns to the premises with a search warrant.

CONCLUSION

For all the reasons stated above, the United States respectfully submits that the motion to suppress be denied.

Respectfully submitted,

UNITED STATES OF AMERICA,
Plaintiff.

JOE W. STECHER
United States Attorney

By: s/ Michael P. Norris
MICHAEL P. NORRIS, #17765
Assistant United States Attorney
1620 Dodge Street, Suite 1400
Omaha, Nebraska 68102-1506
(402) 661-3700

CERTIFICATE OF SERVICE

I hereby certify that on September 20, 2007, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which sent notification of such filing to the following: David R. Stickman

s/ Michael P. Norris
MICHAEL P. NORRIS #17765
Assistant United States Attorney